*53-1003675-01*
*8 May 2015*

# Brocade Flow Optimizer

## User Guide

Supporting version 1.0 of Brocade Flow Optimizer

BROCADE

**© 2015, Brocade Communications Systems, Inc. All Rights Reserved.**

ADX, Brocade, Brocade Assurance, the B-wing symbol, DCX, Fabric OS, HyperEdge, ICX, MLX, MyBrocade, OpenScript, The Effortless Network, VCS, VDX, Vplane, and Vyatta are registered trademarks, and Fabric Vision and vADX are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned may be trademarks of others.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein or the computer programs that accompany it.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit http://www.brocade.com/support/oscd.

# Contents


**Preface** ..... **5**
- Document conventions ..... 5
  - Text formatting conventions ..... 5
  - Command syntax conventions ..... 5
  - Notes, cautions, and warnings ..... 6
- Brocade resources ..... 7
- Contacting Brocade Technical Support ..... 7
- Document feedback ..... 8

**Getting Started** ..... **9**
- Introduction to Brocade Flow Optimizer ..... 9
- System Requirements ..... 10
- Limitations ..... 11
- Installing the Software and Starting the Application ..... 12
- Initial Application Configuration ..... 13
  - Enabling OpenFlow on the MLX Router ..... 13
  - Enabling sFlow Services and Registering the sFlow Destination ..... 14
- Common User Tasks ..... 15
  - Starting the Application ..... 15
  - Stopping the Application ..... 15
  - Logging In ..... 16
  - Logging Out ..... 16
  - Checking the Application Version ..... 17
  - Updating the Controller Settings ..... 17

**User Management** ..... **19**
- Adding New Users ..... 19
- Deleting Users ..... 19
- Changing Passwords ..... 20

**Profile Management** ..... **21**
- About Profiles ..... 21
  - Default Profiles ..... 21
  - Custom Profiles ..... 22
- Creating and Editing Profiles ..... 23
  - Large Flow Detection Parameters ..... 23
  - Mitigation Parameters ..... 25
  - Creating Custom Profiles ..... 28
  - Editing Profiles ..... 30
- Changing the Priority of a Profile ..... 33
- Enabling and Disabling Profiles ..... 34

**Real-time Events** ..... **35**

**Web Client** ..... **36**

Login Page....36
Dashboard....37
Overall Traffic Rate....37
Policy Page....41
Add Custom Profile Dialog....42
Edit Profile Dialog....42
Settings Page....43
Add User Dialog....44
Edit User Dialog....44
Events Page....45

**Troubleshooting....47**
If PostgreSQL Installed on Ubuntu....47
If dbinitialization is triggered with permission denied error....47
The Process for Contacting Support....48
Generating Support Save Data....48
Changing the Logging Level....48
Collecting Information to Report an Issue to Support....49
Debugging Support....50
Error Codes....50

# Preface


- Document conventions....5
- Brocade resources....7
- Contacting Brocade Technical Support....7
- Document feedback....8


# Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

## Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

| Format | Description |
|---|---|
| **bold** text | Identifies command names |
| | Identifies keywords and operands |
| | Identifies the names of user-manipulated GUI elements |
| | Identifies text to enter at the GUI |
| *italic* text | Identifies emphasis |
| | Identifies variables |
| | Identifies document titles |
| `Courier font` | Identifies CLI output |
| | Identifies command syntax examples |

## Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

| Convention | Description |
|---|---|
| **bold** text | Identifies command names, keywords, and command options. |
| *italic* text | Identifies a variable. |
| value | In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, **--show** WWN. |

| Convention | Description |
|---|---|
| [ ] | Syntax components displayed within square brackets are optional.<br>Default responses to system prompts are enclosed in square brackets. |
| { **x** \| **y** \| **z** } | A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.<br>In Fibre Channel products, square brackets may be used instead for this purpose. |
| **x** \| **y** | A vertical bar separates mutually exclusive elements. |
| < > | Nonprinting characters, for example, passwords, are enclosed in angle brackets. |
| ... | Repeat the previous element, for example, *member*[*member*...]. |
| \ | Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash. |

## Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

**NOTE**
A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

**ATTENTION**
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

**CAUTION**
**A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.**

**DANGER**
***A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.***

# Brocade resources

Visit the Brocade website to locate related documentation for your product and additional Brocade resources.

You can download additional publications supporting your product at www.brocade.com. Select the Brocade Products tab to locate your product, then click the Brocade product name or image to open the individual product page. The user manuals are available in the resources module at the bottom of the page under the Documentation category.

To get up-to-the-minute information on Brocade products and resources, go to MyBrocade. You can register at no cost to obtain a user ID and password.

Release notes are available on MyBrocade under Product Downloads.

White papers, online demonstrations, and data sheets are available through the Brocade website.

# Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online, by telephone, or by e-mail. Brocade OEM customers contact their OEM/Solutions provider.

## Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to http://www.brocade.com/services-support/index.html.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

| Online | Telephone | E-mail |
|---|---|---|
| Preferred method of contact for non-urgent issues:<br>• My Cases through MyBrocade<br>• Software downloads and licensing tools<br>• Knowledge Base | Required for Sev 1-Critical and Sev 2-High issues:<br>• Continental US: 1-800-752-8061<br>• Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33)<br>• For areas unable to access toll free number: +1-408-333-6061<br>• Toll-free numbers are available in many countries. | support@brocade.com<br>Please include:<br>• Problem summary<br>• Serial number<br>• Installation details<br>• Environment description |

## Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/Solution Provider, contact your OEM/Solution Provider for all of your product support needs.

- OEM/Solution Providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/Solution Provider.

- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/Solution Provider.

# Document feedback

To send feedback and report errors in the documentation you can use the feedback form posted with the document or you can e-mail the documentation team.

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. You can provide feedback in two ways:

- Through the online feedback form in the HTML documents posted on www.brocade.com.
- By sending your feedback to documentation@brocade.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

# Getting Started

Before you can begin using the Brocade Flow Optimizer application, you need to complete some preliminary tasks, including installing the application software and the initial configuration.

You should also become familiar with some basic tasks that you will perform on a regular basis.


- System Requirements on page 10
- Installing the Software and Starting the Application on page 12
- Initial Application Configuration on page 13
- Common User Tasks on page 15


# Introduction to Brocade Flow Optimizer

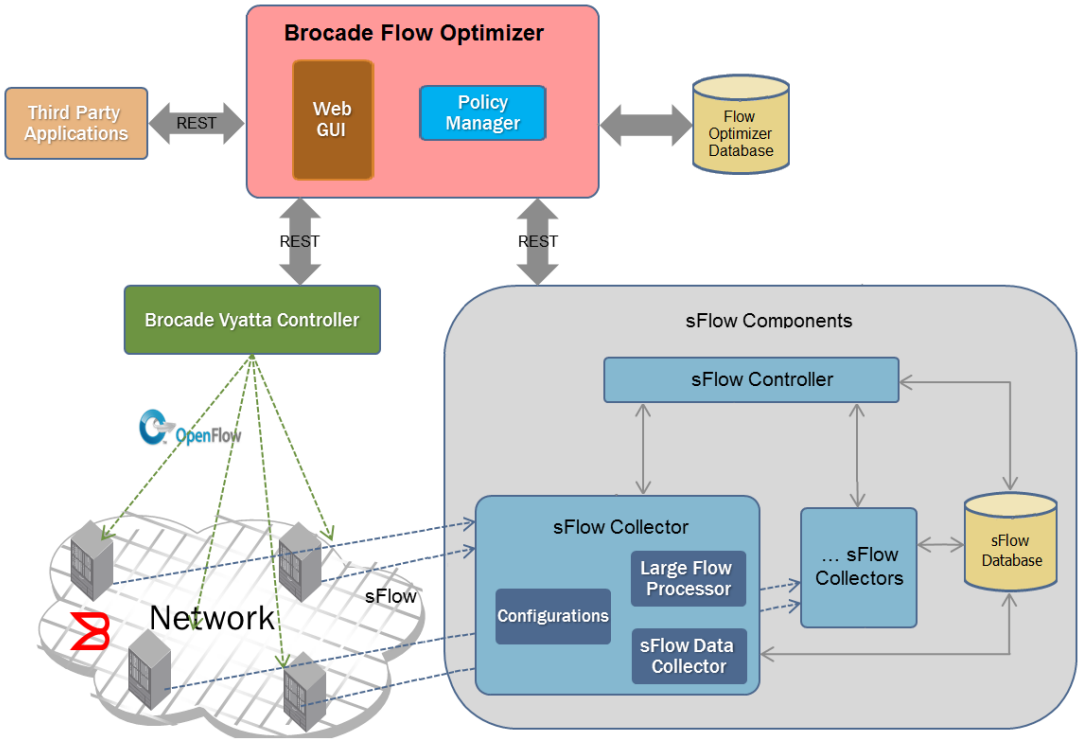
The Brocade Flow Optimizer application is designed to enable you to optimize the traffic flows on your network by providing you with the ability to monitor and control flows that exceed the bandwidth utilization you have established for the flows.

Monitoring traffic flows enables you to identify different types of volumetric traffic that exceed the bandwidth utilization thresholds you have established for the traffic. Once the out-of-range volumetric traffic has been identified, you can enforce your traffic management policy by choosing to drop, redirect, or meter the out-of-range volumetric traffic.

The Brocade Flow Optimizer application monitors sFlow traffic on OpenFlow-enabled ports using the Helium version of the Brocade Vyatta Controller (BVC), or the community Helium OpenDaylight (ODL) controller. The application provides configurable traffic monitoring templates (called profiles) that you use to monitor different types of traffic. It also provides configurable parameters that enable you to set thresholds for the different types of volumetric traffic and to specify the mitigation action for each traffic type.

The application provides a dashboard that enables you to easily view real-time volumetric traffic, real-time events, and the current set of profiles that are available for monitoring traffic. The dashboard also provides access to the options used to configure and edit traffic profiles.

The following figure shows the basic architecture of a typical system implementation of the Brocade Flow Optimizer application.




# System Requirements

Before you can install and use the Brocade Flow Optimizer, you must have certain system software installed.

**NOTE**
Be sure to follow the instructions provided with any software you need to download and install.

## Host Server

**Operating System**

Linux (one of the following):

- Ubuntu 14.0.4 (64 Bit)
- CentOS 7

**Memory** 8GB RAM

**Hard Disk Drive** 64GB of free HDD space

Server needs to have In Band connectivity to MLX device for receiving sFlow packets.

## Hardware

| |
|---|
| FastIron ICX 6610 device |
| NetIron MLXe device |

## Software

| |
|---|
| MLX NetIron firmware, version NI 5.8aa. Download the NetIron firmware from http://www.my.brocade.com. |

**NOTE**
Be sure to follow the upgrade instructions in the *NetIron Upgrade Guide*. Go to http://www.my.brocade.com to download the guide. The guide is for NetIron version 5.7. The instructions are correct and can be used to upgrade to version 5.8.

| |
|---|
| ICX FastIron firmware, version FI 08.0.30 |

## Browser

| |
|---|
| Google Chrome |

## Controller

| | |
|---|---|
| Brocade Vyatta Controller (version 1.3.0) | Go here to download the software: http://www.brocade.com/products/all/software-defined-networking/brocade-vyatta-controller/index.page |
| OpenDaylight (ODL) | ODL Helium-SR2 |

# Limitations

This release of the Brocade Flow Optimizer has the following limitations:

## Flows

The known limitations for this release are:

- The same metered flow cannot be configured on multiple ingress ports. You can configure multiple, independent metered flows on a single ingress port.
- Metered flows are not removed when the bandwidth utilization falls below the Threshold value you specified for the flow. To remove the metered flow, you must disable or delete the profile.

## Profiles

The known limitations for this release are:

- Editing, disabling, or deleting a profile resets the flows defined in the profile.

# Installing the Software and Starting the Application

The steps you use to install the Brocade Flow Optimizer software are the same, regardless of your operating system. The application software is a single archive distributable (.tar), which you need to extract and install on your host server. Once you complete the installation, you need to complete the initial configuration of the application before you can begin using the Brocade Flow Optimizer.

**Pre-requisites:** Make sure that:

- All of the required software is installed (see System Requirements on page 10 for the required software).
- You have downloaded the Brocade Flow Optimizer application software (*Flowoptimizer_<version>_rc_<build#> -distribution.tar*).
- You have extracted the tar archive to the directory where you want the application files to be installed. This will be the home folder for the application.

**NOTE**
When you start the application for the first time, you must set the values of parameters to match the settings of your Controller installation (step 4 and 5). The only other time you need to set these parameter values is if you change the configuration of your Controller.

Complete these steps to start the application.

1. Go to the home directory for the application software distributable archive.
2. Go to bin folder.
3. Use one of the following commands to run the **startservice** script (this starts the application):
   - **sh startservice**
   - **./startservice**
4. Set the values of the following parameters to match the settings of your Controller installation:
   - Controller IP
   - Controller Username
   - Controller Password
   - Device IP list

   **NOTE**
   To specify multiple devices, enter the device IP addresses in comma-separated format.
5. Verify that the values you specified in the previous step are correct, and then enter your changes. A prompt appears asking you if you want to continue with the configuration.
6. Press **Y** to continue.
   The application server is started.

# Initial Application Configuration

Once you have completed the installation of the required software and the Brocade Flow Optimizer application software, you need to configure the system for use.

The system configuration involves the following basic tasks:


- Enabling OpenFlow on the MLX Router on page 13
- Enabling sFlow Services and Registering the sFlow Destination on page 14


## Enabling OpenFlow on the MLX Router

Before you can begin using the application, you must enable OpenFlow on the MLX router, which involves specifying the OpenFlow Controller IP address and specifying maximum allowable number of OpenFlow entries for total OpenFlow entries, protected and unprotected vlan entries, and the maximum number of layer 2, layer 3, or layer 2 and 3 entries.

**Pre-requisites:** Make sure you have completed the installation of the Brocade Flow Optimizer application software.

1. Telnet or SSH into the router and get to the Configure Terminal mode.
   NetIron MLX-4 Router>enable

```
NetIron MLX-4 Router>enable
NetIron MLX-4 Router#configure terminal
NetIron MLX-4 Router(config)#
```

2. Enable OpenFlow Version 1.3 and configure the OpenFlow Controller IP address. The Controller IP address used in this example is 10.1.2.11.

```
NetIron MLX-4 Router(config)#openflow enable ofv130
NetIron MLX-4 Router(config)#openflow controller ip-address 10.1.2.11 no-ssl port
6633
```

3. Enable OpenFlow hybrid port mode on the desired interfaces.

```
NetIron MLX-4 Router(config)#interface ethernet 1/1

NetIron MLX-4 Router(config-if-e10000-1/1)#openflow enable layer23 hybrid-mode
```

**NOTE**
It is recommended that you specify Layer23 hybrid-mode.

4. Set the system maximum (system reload is required once you change the system maximum values). The system maximum values are:

   - OpenFlow entries

```
NetIron MLX-4 Router(config)#system-max  openflow-flow-entries <Valid Decimal
Entry>
DECIMAL   Valid range 0 to 65536 (default: 0)
```

   - OpenFlow protected VLAN entries

```
NetIron MLX-4 Router(config)#system-max  openflow-pvlan-entries <Valid Decimal
Entry>
DECIMAL   Valid range 0 to 2048 (default: 0)
```

   - OpenFlow unprotected VLAN entries

```
NetIron MLX-4 Router(config)#system-max  openflow-unprotectedvlan-entries
<Valid Decimal Entry>
DECIMAL   Valid range 0 to 4096 (default: 0)
```

   - Max Np OpenFlow entries

```
NetIron MLX-4 Router(config)#system-max np-openflow-entries layer2or3 |
layer23IPv4 value slot [ i j k | i to z | all].
```

     (Slot number can be any of the valid slot number in the device. For slots, you can provide "all", "slot 1 to 2" and individual slot options.)

One of the following parameters must be specified:

- **layer23IPv4**

  Layer 2 and 3, including L2 and IPv4 flow entries
- **layer23IPv6**

  Layer 2 and 3, including L2 and IPv6 flow entries

5. Reboot the system.

**Next:** Enabling sFlow services and registering the sFlow destination.

# Enabling sFlow Services and Registering the sFlow Destination

Before you can begin using the Brocade Flow Optimizer, you must enable sFlow services and register the application as the destination for the sFlow traffic.

**Pre-requisites:** Make sure that you have enabled OpenFlow on the MLX router.

1. Telnet or SSH into the router and get to the Configure Terminal mode.

```
NetIron MLX-4 Router>enable
NetIron MLX-4 Router#configure terminal
NetIron MLX-4 Router(config)#
```

2. Enable sFlow services and configure sFlow destination (collector) IP address.

   For example, 10.1.1.10 is an In-Band IP address (NIC) for the application, where sFlow packets are received on default port 6343.

```
NetIron MLX-4 Router(config)#sflow enable
NetIron MLX-4 Router(config)#sflow destination <Inband IP Address of the VM where
the app is installed> 6343
```

3. Enable sFlow null0-sampling on the global level.

```
NetIron MLX-4 Router(config)#sflow null0-sampling
```

4. Set the sFlow sampling rate at the recommended rate: 8192.

```
NetIron MLX-4 Router(config)#sflow sample  8192
```

5. Enable sFlow forwarding on all the Ingress ports being monitored for Volumetric flows.

```
NetIron MLX-4 Router(config)#interface ethernet 1/1
NetIron MLX-4 Router(config-if-e10000-1/1)#sflow forwarding
```

   The **show running-configuration** should display the following sFlow configuration on the router.

```
sflow enable
sflow destination 10.1.1.10
sflow null0-sampling
sflow sample 8192
!
router ospf
 area 0.0.0.0
!
interface management 1
 ip address 10.25.225.34/24
 enable
!
interface ethernet 1/1
 enable
 sflow forwarding
```

6. Perform a write memory operation to save the running-configuration to the startup-configuration and retain the changes.

```
NetIron MLX-4 Router(config)#write memory
Write startup-config done.
```

# Common User Tasks

There are some common tasks that you perform on a regular basis as part of day-to-day operations. These tasks can be easily completed using just a few steps.

These basic tasks include:


- Starting the Application on page 15
- Stopping the Application on page 15
- Logging In on page 16
- Logging Out on page 16
- Checking the Application Version on page 17
- Updating the Controller Settings on page 17


## Starting the Application

You can easily start the Brocade Flow Optimizer application using just a few steps.

The application must be installed on the host server, and you must have access to the server. Other than having access to the host server, there are no pre-requisites for starting the application. The following table lists the login pre-requisites by user type:

| User Type | Pre-requisites |
|---|---|
| Administrator | User account (You do not have to create one. When the application is installed on the host server, a default user with the username Administrator is created.) |
| Operator | User account must be created by Administrator. |

**NOTE**
If you are starting the application for the first time, do not use this procedure. Use the procedure in Installing the Software and Starting the Application on page 12.

Complete these steps to start the application.

1. Go to the home directory (where the application files were installed).
2. Open the bin folder.
3. Use one of the following commands to run the **startservice** script (this starts the application):
   - **sh startservice**
   - **./startservice**

## Stopping the Application

You can easily stop the Brocade Flow Optimizer application using just a few steps.

1. Go to the home directory (where the application files were installed).
2. Open the bin folder.
3. Use one of the following commands to run the **stopservice** script (this stops the application):

- **sh stopservice**
- **./stopservice**

A message appears indicating that the application was stopped successfully.

# Logging In

Before you can begin using the Brocade Flow Optimizer, you must login using the web client. The process is the same regardless of whether you have Administrator or Operator privileges.

You cannot login if the application is not running (started). If you want to login, make sure the application is started.

---

**NOTE**
When the Brocade Flow Optimizer software is installed, an Administrator user is automatically created. If you are an Administrator and are logging in for the first time, use the following credentials:

- **Username** Administrator
- **Password** password

---

Complete these steps to login.

1. Open your browser and point it to the following URL:
   https://<IP address of server>:8089/index.html#/

   ---

   **NOTE**
   The port number must be 8089.

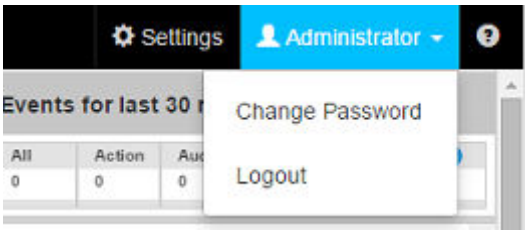
   ---

   Depending on the browser you are using, a page appears with an alert about a security certificate or that the connection may not be secure.
2. Select or click the option to continue with the connection.
   The Login page appears.
3. Type your **Username** and **Password** in the boxes.
4. Press **Enter** or click the **blue arrow**.
   The Dashboard page of the application appears.

# Logging Out

To end your current Brocade Flow Optimizer session, logout using the web client. The process is the same regardless of whether you have Administrator or Operator privileges.

1. Go to the Dashboard page.
2. Click on your **username** at the top-right of the page (next to the Settings tab), then choose **Logout**.



The Dashboard page closes and the Login page appears.

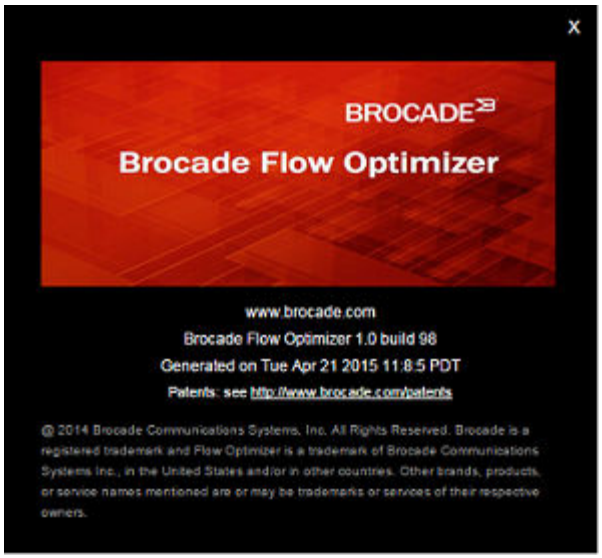
3. (Optional) Close your browser.

## Checking the Application Version

You can easily find which version of the Brocade Flow Optimizer you are using.

Complete these steps to find version information.

1. Login to the application.
2. On the Login page, click the **question mark icon** and choose **About**.
   The About dialog appears showing the version, build, and the time of installation.


BROCADE
Brocade Flow Optimizer
www.brocade.com
Brocade Flow Optimizer 1.0 build 98
Generated on Tue Apr 21 2015 11:8:5 PDT
Patents: see http://www.brocade.com/patents
© 2014 Brocade Communications Systems, Inc. All Rights Reserved. Brocade is a registered trademark and Flow Optimizer is a trademark of Brocade Communications Systems Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned are or may be trademarks or services of their respective owners.

## Updating the Controller Settings

When changes in the system configuration impact the Controller settings defined in the Brocade Flow Optimizer application, you must update the Controller settings in the application. You can use a script provided with the application software to complete the update.

Changes to any of the following require that you update the Controller settings in the application:

- Controller IP
- Controller Username
- Controller Password
- Device IP list

**NOTE**
You use different commands to update the Controller settings. The various commands are listed in the steps to update the settings.

Complete these steps to update the Controller settings.

1. Go to the home directory for the application software distributable archive.
2. Go to bin folder.

3. Use one of the following commands to open the Help so you can find the syntax to use the script to update the configuration:
   - **sh updateconfig --help**
   - **./updateconfig --help**
4. Based on the changes you need to make, use one of the following commands:
   - Use the **sh updateconfig [ -c | -d ]** command to update the Controller IP, username, password, and then update (add or delete) the device IP list.
   - Use the **sh updateconfig** command to update the Controller IP, username, password, and the device IP list at the same time.
   - Use the **sh updateconfig -c** command to update only the Controller IP, username, password (the device IP list is not updated).

     A prompt appears asking you if you want to continue the configuration. Press **Y** to continue updating the Controller settings, or **N** to cancel your updates.
   - Use the **sh updateconfig -d** command to update only the device IP list (the Controller IP, username, and password are not updated).

     A prompt appears asking you if you want to continue the configuration. Press **Y** to update the device IP list, or press **N** to finish the configuration.

# User Management

The Brocade Flow Optimizer application enables you to manage system users to ensure you can create and maintain user accounts as needed.

The different types of user management tasks include:


- Adding New Users on page 19
- Deleting Users on page 19
- Changing Passwords on page 20


# Adding New Users

You can add new users as part of your user management tasks. You must have Administrator privileges to add new users.

The process for adding a new user involves specifying the name (username) and password for the user. Once the new user is added, they can use the Brocade Flow Optimizer application to:

- View the graphs and tables of real-time traffic monitoring data.
- View real-time events.
- Change their own password.

**NOTE**
By default, all new users added by the Administrator have Operator privileges. Users with Operator privileges cannot modify the system configuration or controller settings, add or delete new users, create or edit profiles, or change the passwords of other users.

Use this procedure to add a new user.

1. Go to the Dashboard page.
2. Click the **Settings** tab.
   The list of current users appears.
3. Click the **+ Add new user** link (above the list of users).
   The **Add New User** dialog appears.
4. Type the name (username) and password for the user in the text boxes.
5. Click **OK**.
   The new user is added to the list of current users.

# Deleting Users

You can delete current users as part of your user management tasks. You must have Administrator privileges to add new users.

The process for deleting a user involves selecting the user by name (username) and deleting them. Once the user is deleted, they cannot login to use the Brocade Flow Optimizer application.

**NOTE**
If you delete a user that is logged in, their session is interrupted and they are re-directed to the login page. If they try to login, they are denied access.

Use this procedure to delete a user.

1. Go to the Dashboard page.
2. Click the **Settings** tab.
   The list of current users appears.
3. Locate the user you want to delete, and click the **Delete** option for the user (on the right side of the table).
   A message appears asking you to confirm that you want to delete the user.
4. Do one of the following:
   - Click **OK** to delete the user.
   - Click **Cancel** if you do not want to delete the user.

# Changing Passwords

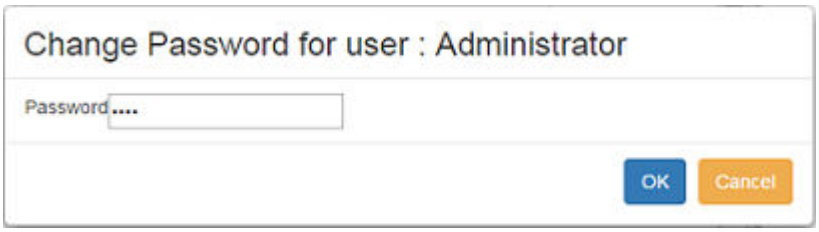
The Brocade Flow Optimizer enables users to changes passwords as part of your user management and system security tasks.

All users can change their own password. Only a user with Administrator privileges can change the passwords of other users (Operator). If you are logged in and you or the system Administrator changes your password, you will automatically be logged out.

Complete these steps to change a password:

**NOTE**
If you want to change your own password, start at step 2. If you have Administrator privileges and want to change the password of another user, start at the beginning of the procedure (step 1).

1. (Administrator only) Login as the user for which you want to change the password.
2. Login using your current credentials.
3. At the Dashboard page, click on the **username** at the top-right of the page (next to the Settings tab), then choose **Change Password**.
   The Change Password dialog appears.




4. Type your new password in the **Password** box, then click **OK**.
   The password is changed.

# Profile Management

Profiles are the main components of your traffic management policy enforcement. You manage the profiles in your traffic management policy by configuring profiles, modifying (editing) profiles, and enabling or disabling profiles.

You use the Policy page of the application to view the current profiles in your traffic management policy and to open the dialogs you use to configure, edit, and enable or disable profiles.

# About Profiles

A profile is a configurable template you use to monitor a specific type of traffic. The main purpose of a profile is to enable you to detect traffic that is above the bandwidth utilization threshold established in your traffic policy for that particular type of traffic.

Profiles also enable you to automate the desired mitigation action for any large flow that is detected. Once you configure the mitigation action in the profile, the system automatically executes the action on any large flow that is detected by the profile.

You configure profiles by setting values for profile parameters that determine:

- The network layer or layers at which traffic is inspected during traffic monitoring.
- The conditions that must be met for a flow to be identified as a large flow.
- The type of mitigation action to be taken once a traffic flow is detected. The available mitigation actions vary depending on whether the profile is a default profile or a custom default profile.

## Basic types of profiles

The Brocade Flow Optimizer provides two basic types of profiles you can use to monitor traffic. They are:

- Default profiles (see Default Profiles on page 21).
- Custom profiles (see Custom Profiles on page 22).

## Default Profiles

There are a total of 4 default profiles provided with the application for detecting volumetric traffic on your network. You use these profiles to monitor NTP reflection traffic, DNS reflection traffic, UDP flood traffic, and ICMP Ping flood traffic.

You can enable, disable, and edit default profiles, and you can change the priority of default profiles. You use the Edit Profiles dialog to edit them.

**NOTE**
You cannot delete default profiles, which you can do with custom profiles.

This table lists and describes the default profiles:

| | |
|---|---|
| DNS Reflection | This profile is used to monitor and detect unrequested DNS query responses coming from third party systems (usually name servers). The third party systems are responding to DNS queries sent from a source (or sources) that typically cannot be traced.<br><br>Because the source IP address of the DNS queries is the IP address of the target, the target receives the DNS query responses. The traffic is amplified because the original DNS queries are often sent from multiple machines to numerous third party systems. The result of the amplification is a huge amount of DNS query responses that consume the target's network resources and disrupt the network.<br><br>The mitigation actions available for this profile are Drop, Redirect, and None. |
| NTP Reflection | This profile is used to monitor and detect unrequested responses from NTP servers. The NTP servers are responding to get monlist requests from a source (or sources) that typically cannot be traced. Because the source IP address of the get monlist requests is the IP address of the target, the target receives the responses from the servers. The traffic is amplified because the original get monlist requests are often sent from multiple machines to numerous NTP servers. The result of the amplification is a huge amount of get monlist responses that consume the target's network resources and disrupt the network.<br><br>The mitigation actions available for this profile are Drop, Redirect, and None. |
| ICMP Ping flood | This profile is used to monitor and detect ICMP echo requests (Ping packets) that did not originate in your network. The requests are a continuous series of Ping packets from a source (or sources) that typically cannot be traced. Because the source IP address of the ICMP echo requests is the IP address of the target, the target host receives the ICMP echo requests and responds with ICMP echo replies. The network becomes overloaded with the exchange of illegitimate ICMP echo and reply messages, which can result in a loss of transmission speed and general performance, and even connectivity issues.<br><br>The mitigation actions available for this profile are Drop, Redirect, and None. |
| UDP flood | This profile is used to monitor and detect illegitimate IP packets that contain UDP datagrams that are not associated with network applications. Typically, the traffic is directed randomly at ports on the target host, which checks the network for applications associated with the UDP datagrams. Because no association exists, the target then responds with destination unreachable messages. The target host becomes overloaded with the exchange of illegitimate IP packets and destination unreachable replies, which prevents it from responding to other network clients.<br><br>The mitigation actions available for this profile are Drop, Redirect, and None. |

## Custom Profiles

The Brocade Flow Optimizer a highly configurable type of profile (called a custom profiles) that you can use along with the default profiles to enforce your traffic management policy.

Like default profiles, custom profiles are designed to enable you to detect large flows and apply mitigation actions to flows that have been detected as large flows. Custom profiles use the traffic detection and mitigation action parameters used in default profiles. However, custom profiles offer a meter (rate-limiting) mitigation action that is not available with default profiles. You can also specify network layer options, which are not available for default profiles.

You can enable, disable, and edit custom profiles, and you can change the priority of custom profiles. You use the Add Custom Profile dialog to create new custom profiles, and the Edit Custom Profiles dialog to edit them.

**NOTE**
You must have Administrator privileges to create, modify, or delete custom profiles.

# Creating and Editing Profiles

The Brocade Flow Optimizer enables you to create and edit profiles to ensure you effectively enforce your traffic management policy.

Although you can edit both default and custom profiles, you can create only custom profiles. Custom profiles are highly configurable: you can create as many variations as you need to effectively enforce your traffic management policy.

**NOTE**
You must have Administrator privileges to create or edit profiles.

The following table lists the types of create and delete operations that can be performed based on the profile type:

| Type | Create | Edit |
|---|---|---|
| Custom | Yes<br>You can create as many custom profiles as you need. | Yes<br>You can modify all of the settings of a custom profile (including the profile name). |
| Default | No | Yes<br>You can modify the mitigation settings of default profiles. You cannot modify the large flow detection settings or the profile name. |

## Changing the priority profile

You can change the priority (ranking of a profile). Changing the priority of profiles enables you to manage the order in which profiles are validated when you monitor traffic. You can change the priority of a profile directly from the Policy page.

## Deleting custom profiles

You can delete custom profiles as part of your profile management tasks. Deleting custom profiles enables you to remove profiles that you no longer use to enforce your traffic management policy. You can delete custom profiles directly from the Policy page.

**NOTE**
You cannot delete default profiles.

## Large Flow Detection Parameters

The large flow detection parameters are configurable parameters that determine which traffic layer or layers are inspected during traffic monitoring. This enables you to define custom profiles you can use to effectively enforce your traffic management policy.

You must configure these parameters when you create new custom profiles. If you need to change the settings to adapt to changes in your traffic management policy, you can edit these settings. The large

flow detection settings are grouped based the network layer that corresponds to the options available in each group. The groups are layer 2 (L2), layer 3 (L3), and layer 4 (L4).

**NOTE**
You do not configure the large flow detection settings for default profiles. These settings are pre-defined in the default profiles that are provided with the Brocade Flow Optimizer software and cannot be changed.

To ensure that the settings you enter are accepted and take effect, make sure that you enter all of the values correctly. The following table lists the requirements for specifying the large flow detection parameter settings.

| Layer | Attribute | Description | Input Format | Requirement |
|---|---|---|---|---|
| L2 | SRC MAC | Source MAC address | 00:00:00:00:00:00 | Valid MAC address in 6 tuples separated by : |
| L2 | DST MAC | Destination MAC address | 00:00:00:00:00:00 | Valid MAC address in 6 tuples separated by : |
| L2 | In VLAN | Ingress Vlan ID | Comma separated Vlan ID's | The Vlan ID's must be configured on the device.<br><br>**NOTE**<br>If you configure this parameter, you must also configure the L2 802.1q parameter. |
| L2 | 802.1q | Vlan Priority | Value from 1 to 7 | <br><br>**NOTE**<br>If you configure this parameter, you must also configure the L2 In VLAN parameter. |
| L3 | Source IP V4 | IPV4 source IP address | Valid IPV4 address. Can use subnet mask or arbitrary bitmask | Combination of IPV4 and IPV6 is not allowed. You must select either IPV4 source and destination, or IPV6 source and destination. |
| L3 | Destination IP V4 | IPV4 destination IP address | Valid IPV4 address. Can use subnet mask or arbitrary bitmask | Combination of IPV4 and IPV6 is not allowed. You must select either IPV4 source and destination, or IPV6 source and destination. |
| L3 | Source IP V6 | IPV6 source IP address | Valid IPV6 address. Can use subnet mask or arbitrary bitmask | User can use subnet mask or arbitrary bitmask in CIDR format. For example:<br>• ipv6: 2001:cdba:9abc:5678::/64<br>• ipv4: 10.3.4.5 or 10.3.4.5/32 |
| L3 | Destination IP V6 | IPV6 destination IP address | | |
| L3 | IP protocol | IP protocol | TCP, UDP, or ICMP | You must select the protocol from the list. |

| Layer | Attribute | Description | Input Format | Requirement |
|---|---|---|---|---|
| L3 | DSCP | Di_ Serv Code Point (part of the IPv4).<br>ToS field or the IPv6 Traffic Class field. | Value from 0 to 63 | |
| L3 | IP Fragment | Yes / No | | **NOTE**<br>This is a detection-only parameter. If you select this option, the **None** mitigation is automatically selected by the system. No mitigation action is applied. |
| L4 | TCP SRC PORT | TCP source port | Valid port number | IP protocol must be selected as TCP. |
| L4 | TCP DST PORT | TCP destination port | Valid port number | IP protocol must be selected as TCP. |
| L4 | UDP SRC PORT | UDP source port | Valid port number | IP protocol must be selected as UDP. |
| L4 | UDP DST PORT | UDP destination port | Valid port number | IP protocol must be selected as UDP. |
| L4 | TCP Flags | TCP Flags | SYN, FIN, ACK, RST, URG, or PSH | TCP Flags<br>IP protocol should be selected as TCP<br>**NOTE**<br>This is a detection-only parameter. If you select this option, the **None** mitigation is automatically selected by the system. No mitigation action is applied. |

# Mitigation Parameters

The mitigation parameters are configurable profile parameters that determine the conditions that must be met before traffic flows are identified as large flows, and the action taken on the large flows.

Most of these parameters are common to both default profiles and custom profiles. You configure these parameters when:

- You create new custom profiles.
- You edit custom profiles or default profiles.

Most of these parameters are common to both default profiles and custom profiles.

The mitigation parameters are:

- Observation time
- Threshold (Mbps)
- Action

### *Observation time*

The following table lists the description of this mitigation parameter and any options available for this parameter.

| Description |
|---|
| The amount of time (in seconds) that the application monitors the bandwidth utilization of traffic targeted to a single destination before marking it as a large flow. If the bandwidth utilization exceeds the Threshold value for the duration of the Observation time, the flow is identified as a large flow. |

**NOTE**
When the bandwidth utilization of traffic that has been identified as a large flow falls below the Threshold value for the duration of the Observation time, the traffic is no longer identified as a large flow. The traffic is then either dropped or rate-limited (metered) based on the mitigation action selected for the profile.

### *Threshold (Mbps)*

The following table lists the description of this mitigation parameter and any options available for this parameter.

| Description |
|---|
| The bandwidth utilization threshold (in Mbps) used to identify a flow as a large flow. If the bandwidth utilization of a flow exceeds the value throughout the Observation time, the flow is marked as a large flow. |

### *Action*

Configuring this mitigation parameter determines which mitigation action is automatically applied by the system to large flows. The options are:

- None (default and custom profiles)
- Drop (default and custom profiles)
- Redirect (default and custom profiles)
- Meter (custom profiles only)

The following table lists the description of this mitigation parameter and any options available for this parameter.

| Action mitigation parameter options |
|---|
| **None**: No mitigation action is taken. Use this to monitor flows without altering the traffic. |
| **Drop**: The flow is blocked. Sampling of sFlow traffic still occurs at the MLX ports even after the traffic is blocked. |

**Redirect**: Traffic is redirected to a port or ports on the device you select to receive the traffic. Use the drop down menu to select the device and ports using these options:

- **Redirect Node**: The IP address of the device you want to receive the redirected traffic flow.
- **Redirect Ports**: The port (or ports) on the device you want to receive the redirected traffic flow. (Make sure you use the OpenFlow ID of the ports. On the MLX, use the **show openflow** interface command to find the port IDs.)

**Meter**: The traffic rate is limited (metered) to the bandwidth utilization you specify using the **Rate Limit Bandwidth** parameter. This action is only available for custom profiles based on matching vlan ids.

You have two options when using the Meter mitigation action. They are **Meter with drop band**, and **Meter with DSCP Remark band**.

**NOTE**
You can use **Meter with drop band** alone. If you want to use the **Meter with DSCP Remark band**, you must use it together with the **Meter with drop band** option.

- **Meter with drop band**

  The flow is metered (rate-limited) to the **Rate Limit Bandwidth** value you specify. All the traffic above the rate limit is dropped.

  If you use this Meter option, you must configure the following:

  - **Ingress Port and Node**: The node IP address and port number of the ingress (input) port of the traffic used to create the flow. Must be a single port.

    **NOTE**
    The ingress port must be part of the vlan you specify using the **Ingress VLAN ID** option.
  - **Ingress VLAN ID**: The vlan ID or IDs for creating the flow. The ingress port must be part of vlan ID you specify. To specify multiple vlans, enter the IDs in comma separated format (ID 1, ID 2, ID 3). If you specify multiple vlans, the large flows are identified separately for each vlan.
  - **Rate Limit Bandwidth**: The bandwidth utilization rate (in Mbps) used to limit the flow. The rate of the flow is limited to the value you specify.
- **Meter with DSCP Remark band**

  The DSCP remark is used to decrease the drop-precedence of the DSCP field in the IP header of the packet. When the system applies the DSCP remark, all packets that exceed the **Remark Rate** you specify are modified. The DSCP precedence value of these packets is set to the **DSCP Precedence** value you specify. You have the option of selecting a node and ports from the node received from the Controller.

  If you use this Meter option, you must configure the following:

  - **DSCP Rate limit**: The maximum bandwidth utilization for the DSCP remark.
  - **DSCP Precedence**: The value of the drop-precedence field in the IP header.
  - **Ingress Port and Node**: The node IP address and port number of the ingress (input) port of the traffic used to create the flow. Must be a single port.

    **NOTE**
    The ingress port must be part of the vlan you specify using the **Ingress VLAN ID** option.
  - **Ingress VLAN ID**: The vlan ID or IDs for creating the flow. The ingress port must be part of vlan ID you specify. To specify multiple vlans, enter the IDs in comma separated format (ID 1, ID 2, ID 3). If you specify multiple vlans, the large flows are identified separately for each vlan.

# Creating Custom Profiles

The Brocade Flow Optimizer enables you to create new profiles (called custom profiles) to use along with the default profiles to enforce your network management policy.

You use the Add Custom Profile dialog to create new custom profiles. Once the new custom profile is created, you can easily begin using it to monitor traffic.

When you create new custom profiles, you must configure two basic types of settings. They are:

| | |
|---|---|
| Large flow detection settings | Used to determine the network layer or layers that are inspected during traffic monitoring. |
| Mitigation settings | Used to define the conditions that must be met before a flow is identified as a large flow, and the mitigation action that is applied to large flows. |

**NOTE**
Make sure you are familiar with the large flow detection parameters and mitigation action parameters, see Large Flow Detection Parameters on page 23 and Mitigation Parameters on page 25.

The process for creating a new custom profile involves:

- Naming the profile and entering a description.
- Configuring the large flow detection settings.
- Configuring the mitigation action settings.

Complete these steps to create a new custom profile:

1. Go to the application Dashboard.
2. Make sure the Policy page is selected.
3. Click the **Add Custom Profile** link (near the top left of the page).
   The Add Custom Profile dialog appears.
4. In the **Profile Name** column, type the name for the profile.

   **NOTE**
   The maximum length of the profile name is 128 Character. A profile name can contain only alpha numeric characters and special characters like (- / . / _ / ~).
5. In the **Description** box, type a description for the profile.

   **NOTE**
   Steps **6**, **7**, and **8** are for selecting the network layers for the profile (L2, L3, or L4). You can select any combination of layers, but you must select at least one layer. For each layer you select, you must specify the source and destination addresses, ports, and any other mandatory items.
6. (Optional) In the **Large flow detection settings** section, select the **L2** checkbox.
   a) Specify the **Source MAC** address for the flow.
   b) Specify the **Destination MAC** address for the flow.
   c) Specify the **Ingress Vlan ID** for the flow.
   d) Specify the **VLAN Priority** for the flow.
7. (Optional) In the **Large flow detection settings** section, select the **L3** checkbox.
   a) Specify the **Source IP (IPv4)** address for the flow.
   b) Specify the **Destination IP (IPv4)** address for the flow.

c) Specify the **Source IP (IPv6)** for the flow.
d) Specify the **Destination IP (IPv6)** for the flow.
e) Specify the **IP Protocol** for the flow.

8. (Optional) In the **Large flow detection settings** section, select the **L4** checkbox.
   a) Specify the **TCP Source Port** address for the flow.
   b) Specify the **TCP Destination Port** address for the flow.
   c) Specify the **UDP Source Port** for the flow.
   d) Specify the **UDP Destination Port** for the flow.
   e) Specify the **TCP Flags** for the flow.
9. In the **Mitigation settings** section, enter the amount of time in the **Observation time** box that you want to monitor traffic before a flow is identified as a large flow.
10. In the **Threshold (Mbps)** box, enter the bandwidth utilization threshold (in Mbps) that a flow must exceed before it is a flow is identified as a large flow.
11. Using the **Action** menu, choose one of the following mitigation actions:

- **None** No mitigation action is taken.
- **Drop** The flow is blocked.
- **Redirect** Traffic is redirected to a port or ports on the device you select to receive the traffic. Use the drop down menu to select the device and ports using these options:
  - **Redirect Node**: The IP address of the device you want to receive the redirected traffic flow.
  - **Redirect Ports**: The port (or ports) on the device you want to receive the redirected traffic flow. (Make sure you use the OpenFlow ID of the ports. On the MLX, use the **show openflow** interface command to find the port IDs.)

**NOTE**
The next action (Meter) applies only to custom profiles based on matching vlan ids. If you are changing the settings for a default profile, you have completed the procedure. Click **OK** to save the changes.

- **Meter** The traffic rate is limited (metered) to the bandwidth utilization you specify using the **Rate Limit Bandwidth** parameter. Choose either the **Meter with drop band** or the **Meter with DSCP Remark band** option.

**NOTE**
You can use **Meter with drop band** alone. If you want to use the **Meter with DSCP Remark band**, you must use it together with the **Meter with drop band** option.

  - **Meter with drop band**: The flow is metered (rate-limited) to the **Rate Limit Bandwidth** value you specify. All the traffic above the rate limit is dropped. You must configure the following:
    - **Ingress Port and Node**: The node IP address and port number of the ingress (input) port of the traffic used to create the flow. Must be a single port.

**NOTE**
The ingress port must be part of the vlan you specify using the **Ingress VLAN ID** option.

- **Ingress VLAN ID**: The vlan ID or IDs for creating the flow. The ingress port must be part of vlan ID you specify. To specify multiple vlans, enter the IDs in comma separated format (ID 1, ID 2, ID 3).
- **Rate Limit Bandwidth**: The bandwidth utilization rate (in Mbps) used to limit the flow. The rate of the flow is limited to the value you specify.

- **Meter with DSCP Remark band**: The DSCP remark is used to decrease the drop-precedence of the DSCP field in the IP header of the packet. Packets that exceed the **Remark Rate** you specify are modified, and the DSCP precedence value is set to the **DSCP Precedence** value you specify. You must configure the following:
  - **DSCP Rate limit**: The maximum bandwidth utilization for the DSCP remark.
  - **DSCP Precedence**: The value of the drop-precedence field in the IP header.
  - **Ingress Port and Node**: The node IP address and port number of the ingress (input) port of the traffic used to create the flow. Must be a single port.

**NOTE**
The ingress port must be part of the vlan you specify using the **Ingress VLAN ID** option.

- **Ingress VLAN ID**: The vlan ID or IDs for creating the flow. The ingress port must be part of vlan ID you specify. To specify multiple vlans, enter the IDs in comma separated format (ID 1, ID 2, ID 3).

12. Click **OK** to save the changes.
    The profile is created and appears in the list of profiles on the Policy page.

# Editing Profiles

The Brocade Flow Optimizer enables you to edit profiles to ensure your current set of profiles can be used to effectively enforce your network management policy. You can edit both default profiles and custom profiles.

The types of changes you can make to a profile varies depending on the profile type (default or custom). The major task when editing profiles involves modifying the values of profile parameters.

The following table lists the types of modifications that are possible when you edit profiles.

| Profile Type | Configurable Settings | Steps |
|---|---|---|
| Custom | Large Flow Detection Settings | See Changing Large Flow Detection Parameter Settings on page 31 |
| | Mitigation Settings | See Changing Mitigation Parameter Settings on page 32 |
| Default | Mitigation Settings | See Changing Mitigation Parameter Settings on page 32 |

## *Changing Large Flow Detection Parameter Settings*

You can modify the large flow detection parameter settings of custom profiles. This enables you to change the profiles as needed to adapt to changes in your network traffic management policy. These settings determine which traffic layer or layers that are inspected during traffic monitoring.

You use the Edit Custom Profile dialog to change the large flow detection settings of custom profiles. The detailed steps you use to change these settings are the same as the steps used to define these settings when you create custom profiles.

**NOTE**
Make sure you are familiar with the requirements for configuring the network layer settings (for example, MAC addresses need to be entered in a specific format). See Large Flow Detection Parameters on page 23 for details.

Complete these steps to change the large flow detection settings of a custom profile:

1. Go to the application Dashboard.
2. Make sure the Policy page is selected.
3. In the **Profile Name** column, find the name of the custom profile you want to edit.
4. In the Options column for the profile, click **Edit**.
   The Edit Custom Profile dialog appears.

**NOTE**
Steps **5**, **6**, and **7** are for selecting the network layers for the profile (L2, L3, or L4). You can select any combination of layers, but you must select at least one layer. For each layer you select, you must specify the source and destination addresses, ports, and any other mandatory items.

5. (Optional) In the **Large flow traffic detection settings** section, select the **L2** checkbox.
   a) Specify the **Source MAC** address for the flow.
   b) Specify the **Destination MAC** address for the flow.
   c) Specify the **Ingress Vlan ID** for the flow.
   d) Specify the **VLAN Priority** for the flow.
6. (Optional) In the **Large flow traffic detection settings** section, select the **L3** checkbox.
   a) Specify the **Source IP (IPv4)** address for the flow.
   b) Specify the **Destination IP (IPv4)** address for the flow.
   c) Specify the **Source IP (IPv6)** for the flow.
   d) Specify the **Destination IP (IPv6)** for the flow.
   e) Specify the **IP Protocol** for the flow.
7. (Optional) In the **Large flow traffic detection settings** section, select the **L4** checkbox.
   a) Specify the **TCP Source Port** address for the flow.
   b) Specify the **TCP Destination Port** address for the flow.
   c) Specify the **UDP Source Port** for the flow.
   d) Specify the **UDP Destination Port** for the flow.
   e) Specify the **TCP Flags** for the flow.
8. Click **OK** to save the changes.

(Optional) If you want to change the mitigation settings of the profile, see Changing Mitigation Parameter Settings on page 32.

## *Changing Mitigation Parameter Settings*

You can modify the mitigation parameter settings of profiles. This enables you to change profiles as needed to adapt to changes in your network traffic management policy. These settings determine the conditions that must be met before a flow is detected as a large flow, and the mitigation action taken once a flow is detected as a large flow.

You can use this procedure to modify the mitigation settings of custom profiles or default profiles.

**NOTE**
For detailed descriptions of the mitigation parameters, see Mitigation Parameters on page 25.

Use this procedure to modify the mitigation settings.

1. Go to the application Dashboard.
2. Make sure the Profile page is selected.
3. In the **Profile Name** column, find the name of the profile you want to edit.
4. In the Options column for the profile, click **Edit**.
   If you are editing a default profile, the Edit Profile dialog appears. If you are editing a custom profile, the Edit Custom Profile dialog appears.
5. In the **Mitigation settings** section, enter the amount of time in the **Observation time** box that you want to monitor traffic before a flow is identified as a large flow.
6. In the **Threshold (Mbps)** box, enter the bandwidth utilization threshold (in Mbps) that a flow must exceed before it is a flow is identified as a large flow.

   The next step is used to modify the settings for the **Action** parameter. If you want to configure or modify the configuration of the Meter mitigation action, make sure you are familiar with the options for this parameter (see Mitigation Parameters on page 25).
7. Using the **Action** menu, choose one of the following mitigation actions:

   - **None** No mitigation action is taken.
   - **Drop** The flow is blocked.
   - **Redirect** Traffic is redirected to a port or ports on the device you select to receive the traffic. Use the drop down menu to select the device and ports using these options:
     - **Redirect Node**: The IP address of the device you want to receive the redirected traffic flow.
     - **Redirect Ports**: The port (or ports) on the device you want to receive the redirected traffic flow. (Make sure you use the OpenFlow ID of the ports. On the MLX, use the **show openflow** interface command to find the port IDs.)

     **NOTE**
     The next action (Meter) applies only to custom profiles based on matching vlan ids. If you are changing the settings for a default profile, you have completed the procedure. Click **OK** to save the changes.
   - **Meter** The traffic rate is limited (metered) to the bandwidth utilization you specify using the **Rate Limit Bandwidth** parameter. Choose either the **Meter with drop band** or the **Meter with DSCP Remark band** option.

**NOTE**
You can use **Meter with drop band** alone. If you want to use the **Meter with DSCP Remark band**, you must use it together with the **Meter with drop band** option.

- **Meter with drop band**: The flow is metered (rate-limited) to the **Rate Limit Bandwidth** value you specify. All the traffic above the rate limit is dropped. You must configure the following:
  - **Ingress Port and Node**: The node IP address and port number of the ingress (input) port of the traffic used to create the flow. Must be a single port.

    **NOTE**
    The ingress port must be part of the vlan you specify using the **Ingress VLAN ID** option.
  - **Ingress VLAN ID**: The vlan ID or IDs for creating the flow. The ingress port must be part of vlan ID you specify. To specify multiple vlans, enter the IDs in comma separated format (ID 1, ID 2, ID 3).
  - **Rate Limit Bandwidth**: The bandwidth utilization rate (in Mbps) used to limit the flow. The rate of the flow is limited to the value you specify.
- **Meter with DSCP Remark band**: The DSCP remark is used to decrease the drop-precedence of the DSCP field in the IP header of the packet. Packets that exceed the **Remark Rate** you specify are modified, and the DSCP precedence value is set to the **DSCP Precedence** value you specify. You must configure the following:
  - **DSCP Rate limit**: The maximum bandwidth utilization for the DSCP remark.
  - **DSCP Precedence**: The value of the drop-precedence field in the IP header.
  - **Ingress Port and Node**: The node IP address and port number of the ingress (input) port of the traffic used to create the flow. Must be a single port.

    **NOTE**
    The ingress port must be part of the vlan you specify using the **Ingress VLAN ID** option.
  - **Ingress VLAN ID**: The vlan ID or IDs for creating the flow. The ingress port must be part of vlan ID you specify. To specify multiple vlans, enter the IDs in comma separated format (ID 1, ID 2, ID 3).

8. Click **OK** to save the changes.

# Changing the Priority of a Profile

A priority is automatically assigned by the system to a profile when you configure the profile. Default profiles are automatically assigned the highest priority, and custom profiles are automatically assigned the lowest priority.

Profile priority determines the order in which the system validates currently defined profiles when sFlow samples are received. The current priority ranking of the profiles you have configured is reflected in the list of profiles in the Policy page. Profiles higher in the list (at or near the top of the list) have a higher priority than profiles that are further down in the list. Profiles are validated in the order they appear in the list on the Policy page.

You can change the priority by moving one or more profiles up or down in the list. You do this by clicking the **Move up** or **Move down** options for the profile. When a new custom profile is defined, it is

added with least priority and is listed at the bottom. User has to change the priority as per his requirement.

**NOTE**
When the system encounters a profile that matches the configuration of a profile with a higher priority that has already been validated, the lower priority profile is not validated.

# Enabling and Disabling Profiles

You must enable one or more profiles before you can monitor traffic to enforce your traffic management policy. For example, if you want to monitor NTP reflection traffic, you must enable an NTP Reflection profile.

1. Go to the application Dashboard.
2. Make sure the Profile page is selected.
3. In the **Profile Name** column, find the name of the profile you want to enable or disable.
4. In the Options column for the profile, enable or disable the profile by clicking the **Enable** or **Disable** button.
   The status icon next to the name of the profile changes color to reflect the new status (red indicates a status of disabled, green indicates a status of enabled).

# Real-time Events

The Brocade Flow Optimizer provides records two types of real-time events. One type is traffic monitoring events and the other type is audit events. Every event logged by the application has a time stamp, description, and a unique identifier.

Both types of real-time events can be viewed on the Events page, or the Events pane of the Dashboard. The Events page lists events that have occurred over the last few days or more. The Events pane of the Dashboard lists events that have occurred over the last 30 minutes.

The application stores a maximum of 50000 events. Any events beyond the maximum storage capacity are purged nightly from the database.

The different real-time events are:

- **Flow Added:** Indicates that the flow was successfully added to the profile. The profile name appears in the description of the event.
- **Flow Creation Failed:** The flow that was configured and enabled for monitoring could not be generated.
- **Flow Detected:** Indicates that the flow has been detected as a large flow, which means that the flow has exceeded the bandwidth utilization threshold for the flow. The yellow warning icon appears on the left side next to the event.
- **Flow Removed:** Indicates that the flow was successfully removed. Flows are removed if the bandwidth utilization falls below the bandwidth utilization threshold.
- **Flow Removal Failed:** A flow that was detected and should have been removed based on the specified mitigation action could not be removed.
- **Meter Created:** A meter was set up in the system for a flow based on your configuration settings.
- **Meter Deleted:** A meter was set up in the system for a flow based on your configuration settings was successfully deleted.
- **Meter Add / Delete Failed:** A meter that you set up for a flow could not be created, or a meter that you selected for deletion could not be deleted.
- **Mitigated:** A flow that was detected has been mitigated based on the mitigation action you specified for the flow. The different mitigation actions are:
  - **Default profiles:** The mitigation action events are **Drop**, **Redirect**, and **None**.
  - **Custom profiles:** The mitigation action events are **Drop**, **Redirect**, **None**, **Remark**, and **Meter**.
- **Profile Created:** A profile you configured has been created by the system.
- **Profile Deleted:** A profile you deleted from your set of profiles (policy) has been successfully removed from the system.
- **Profile Add / Delete Failed:** A profile that you configured could not be created, or a profile that you selected for deletion could not be deleted.
- **Audit:** The total number of events performed by users (Administrator or Operator) that have been logged during the last 30 minutes of the current session. This includes the changing of controller settings, adding, editing, or deleting profiles, and user management events.

# Web Client

The Brocade Flow Optimizer application provides a browser-based graphical user interface (GUI) client that enables you to view real-time volumetric traffic being monitored by the system and to view real-time events.

The GUI provides access the application dashboard, which you use to view information about traffic flows currently being monitored using profiles. It also contains pages and dialogs that you use to complete tasks that are essential to using the application. The GUI utilizes REST API's exposed by the application.

You can use the various GUI pages and dialogs to:

- View information about traffic flows currently being monitored
- Create and edit traffic profiles, and view profile settings
- View important traffic monitoring events
- Manage system users
- Login and logout

# Login Page

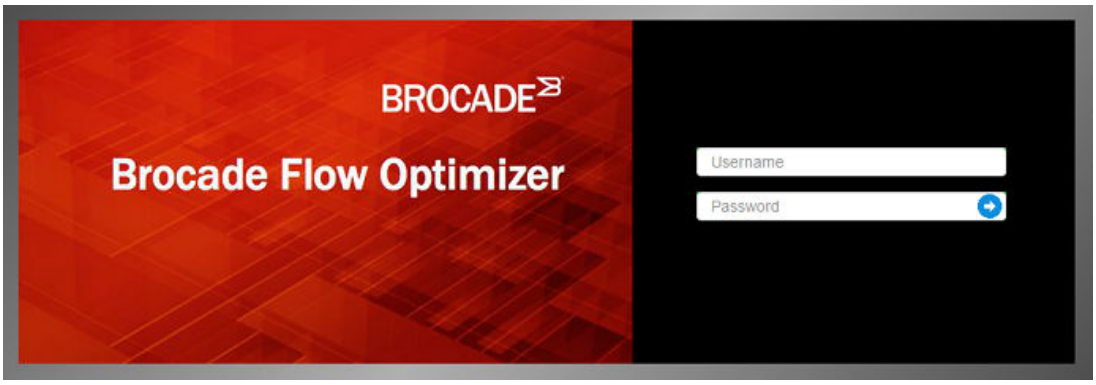
The Login page is used to login to the Brocade Flow Optimizer application on the host server that is running the application. The application must be running to login. If it is not running, you must start the application before you login.

Once you login, the application session starts. If there is no user activity for 30 minutes after the session starts, the session times out (closes), and you must login again.

To login, open your browser and point it to **https://<Server_IP>:8089**.

**NOTE**
The port number must be 8089.

The Login page appears.




Type your username and password in the appropriate boxes, then press **Enter** or click the **blue arrow**.

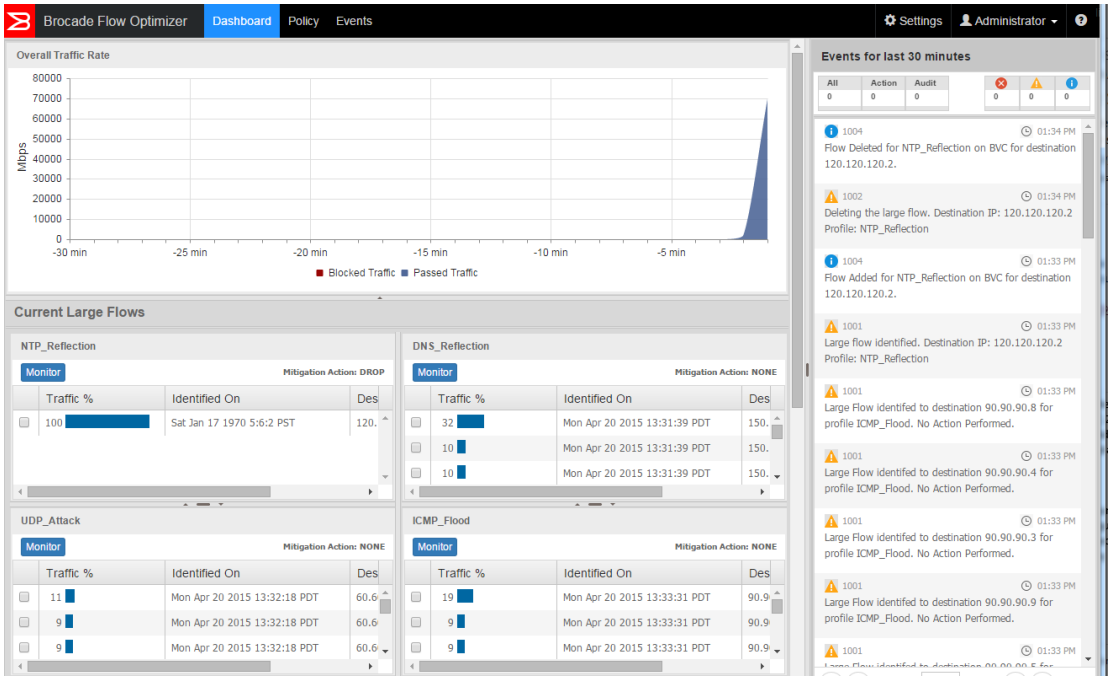
The Dashboard page appears.

# Dashboard

The Dashboard is the main page of the Brocade Flow Optimizer application. It is the page you use to view graphs of real-time data about traffic being monitored and the most recent real-time events.

When you login, the Dashboard page appears showing the Overall Traffic Rate graph, Current Large Flows tables, and the Events pane. The Overall Traffic Rate graph and Current Large Flows tables show traffic monitoring data and the Events section shows traffic monitoring events for the last 30 minutes.

The following figure shows the Dashboard page.



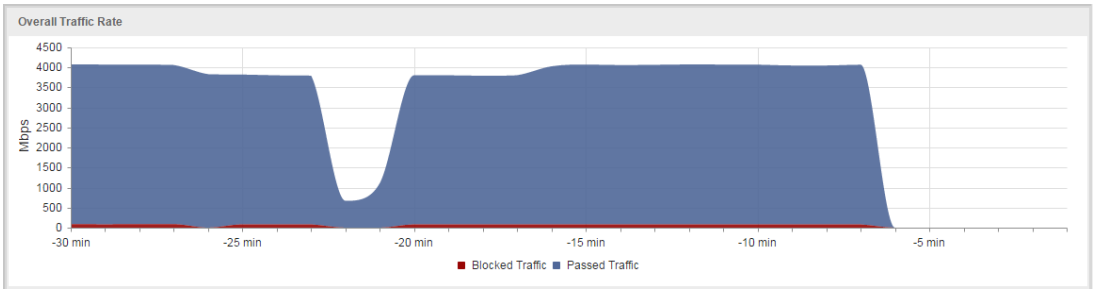

**NOTE**
To view a full history of traffic monitoring events, use the Events page, not the Events section of the Dashboard.

## Overall Traffic Rate

The Overall Traffic Rate is a real-time graph that shows the traffic currently being monitored. It is a stacked graph that gives you a real-time snapshot of the traffic being monitored in one easy-to-read graph. All of the flows being monitored are aggregated into one of the stacks of the graph based on a few basic conditions.

This graph shows the traffic data for last 30 minutes and is refreshed once every minute. The graph continues plotting data if the window is minimized or goes out of focus.

The following figure shows the Overall Traffic Rate graph.




The different stacks represent the following:

| | |
|---|---|
| Blocked Traffic | Large traffic flows (in Mbps) that are being blocked. The traffic is being blocked because the bandwidth utilization of the flows has exceeded the bandwidth utilization threshold, and the Drop mitigation action is being applied to the flows. |
| Passed Traffic | Large traffic flows (in Mbps) that are not being blocked. The traffic is being redirected, remarked, metered, or allowed to pass unaltered because the bandwidth utilization of the flows has exceeded the bandwidth utilization threshold for the flows, and the selected mitigation action is being applied to the flows.<br><br>The mitigation action you have selected in the profile determines whether the flow is being re-directed, remarked, metered, or allowed to pass unaltered. |

The x-axis represents the time stamp (on the application Client), and the y-axis represents the throughput in Mbps. The legend shows how traffic flows are represented in the graph.

## *Current Large Flows*

The Current Large Flows pane of the Dashboard shows the table for each active profile. Traffic flows that have been detected as large flows are listed in the table (each flow appears in its own row in the table).

The data is real-time data, and is refreshed every 15 seconds. The title of each table shows the name of the profile. The mitigation action of the profile is shown to the right of the title bar.

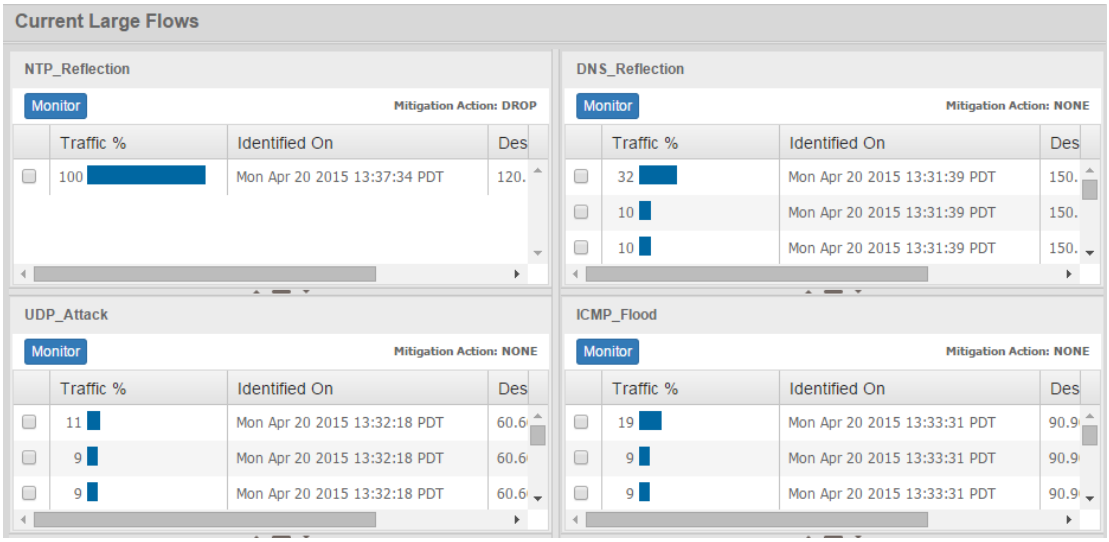
**NOTE**
Click the **Monitor** button in a table to view real-time traffic monitoring data for the profile.

The Current Large Flows tables have the following columns:

- **Traffic %:** The bandwidth utilization of the flow.
- **Identified On:** The time stamp (on the application client) when the flow was detected.
- **Destination:** The destination IP address of the flow. (This only applies to default profiles.)
- **Columns for network attributes:** For custom profiles, columns are used to show the network attributes. (This only applies to custom profiles.)

**NOTE**
If none of the flows being monitored by the profile exceed the bandwidth utilization threshold for the duration of the observation period, no traffic is detected and the table is empty.

The following example shows the tables for the default profiles. In this example, all of the profiles are showing real-time monitoring data.




## *Events Pane*

The Events pane of the Dashboard lists the real-time traffic monitoring events and auditing events that have occurred within the last 30 minutes. The table is automatically updated every 15 seconds with the most recent real-time events.

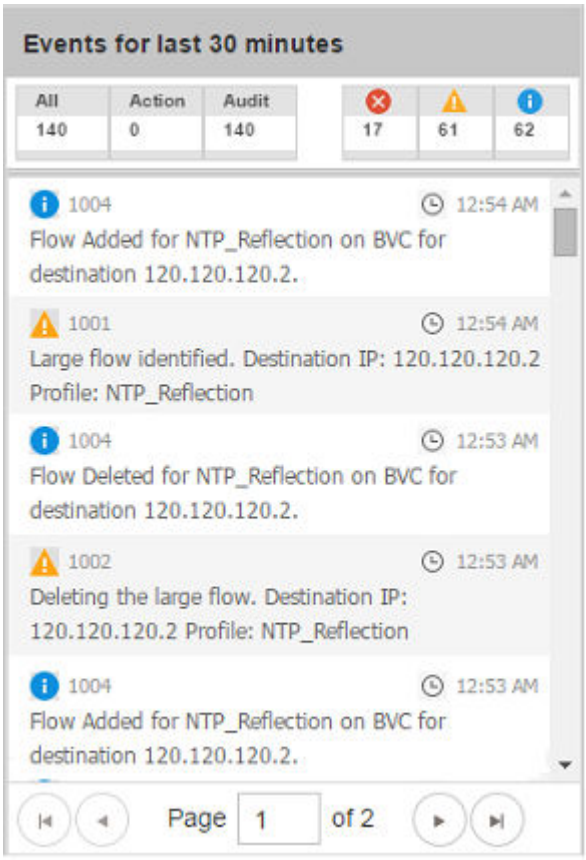
---

**NOTE**
If you want to view events that have occurred over the last few days or more, use the Events page (click on the **Events** tab of the Dashboard).

---

You can scroll through the list to view more events. If you get to the bottom of the list, use the buttons on the bottom of the pane to view the next page of events.

The following figure shows the Events pane.




For each event, the following information is provided in the columns of the Events pane:

- **Severity** The icon at the left of each entry indicates the severity of the event.

| | |
|---|---|
| | Critical event |
| | Warning event |
| | Information event (system-wide events that occur during the processing of flows and application of mitigation actions) |

- **Message ID** The unique identifier for the message. (Shown next to the severity icon.)
- **Time** The time the event occurred (the client time stamp).
- **Description** A brief description of the event.

The Events page also provides counters for real-time events.

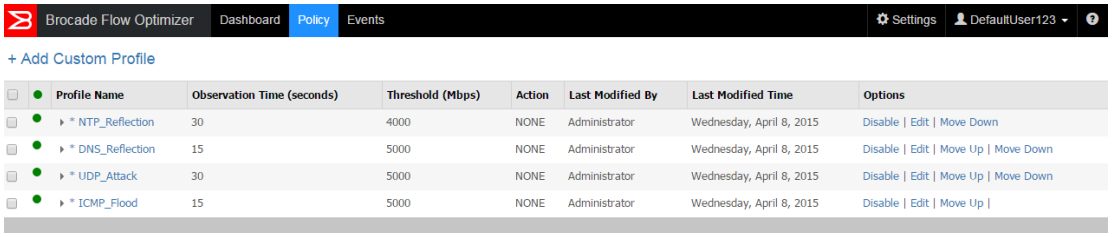
| | |
|---|---|
| All | The total number of events that have been logged during the last 30 of the current session. |
| Action | The total number of events related to monitoring traffic for large flows. These events include the setup of profiles, flows, the detection of large flows, the execution of mitigation actions and more. |

| | |
|---|---|
| Audit | The total number of events performed by users (Administrator or Operator) that have been logged during the last 30 minutes of the current session. This includes the changing of controller settings, adding, editing, or deleting profiles, and user management events. |

# Policy Page

The Policy page of the graphical user interface (GUI) client lists all of the profiles that are available to use to monitor traffic. To view this page, click the **Policy** tab at the top of the Dashboard page.

The following figure shows the Policy page. In this example, the 4 default profiles are shown.


Brocade Flow Optimizer
Dashboard
Policy
Events
Settings
DefaultUser123
+ Add Custom Profile
Profile Name
Observation Time (seconds)
Threshold (Mbps)
Action
Last Modified By
Last Modified Time
Options
* NTP_Reflection 30 4000 NONE Administrator Wednesday, April 8, 2015 Disable | Edit | Move Down
* DNS_Reflection 15 5000 NONE Administrator Wednesday, April 8, 2015 Disable | Edit | Move Up | Move Down
* UDP_Attack 30 5000 NONE Administrator Wednesday, April 8, 2015 Disable | Edit | Move Up | Move Down
* ICMP_Flood 15 5000 NONE Administrator Wednesday, April 8, 2015 Disable | Edit | Move Up |

The green circle icon shown in the second column indicates that the profile is active and is currently being used to monitor traffic. The red circle icon indicates that the profile is inactive and is not currently being used to monitor traffic. In addition to viewing the list of available profiles and profile details, you can open the dialogs you use to edit profiles by using the blue buttons in the Options column.

If you want to change the priority of a profile, you can:

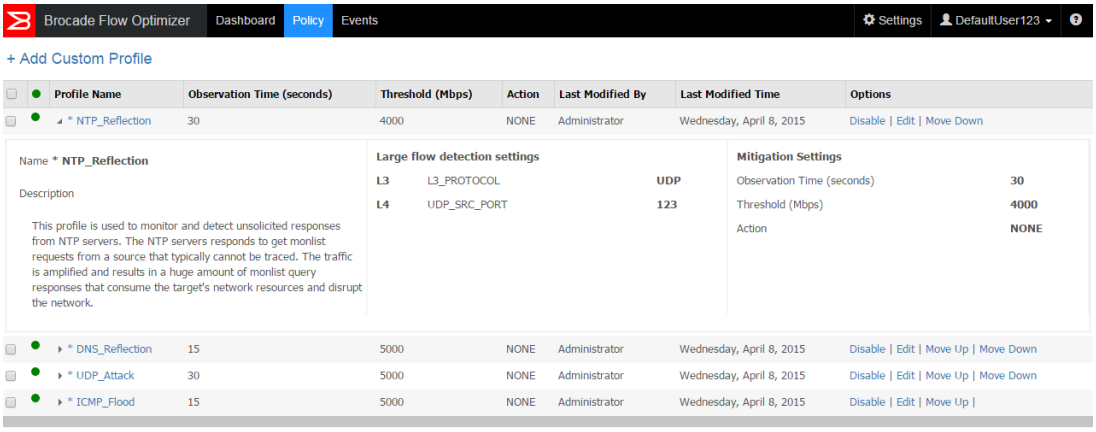
- Increase the priority by clicking the **Move Up** button.
- Decrease the priority of a profile by clicking the **Move Down** button.

You can view the details for a profile by clicking the arrow next to the name of the profile. The details shown include the profile description, the values for the traffic detection parameters, the specified mitigation action, and the time it was last modified.

**NOTE**
You cannot use this view to edit the profile. It is a read-only view of the profile.

When you click **Edit** in the Options column for a profile, all the parameters available for that profile are shown along with the current settings (values) for each parameter.

The following figure shows the expanded view for a profile named NTP Reflection.


Brocade Flow Optimizer
Dashboard
Policy
Events
Settings
DefaultUser123
+ Add Custom Profile
Profile Name
Observation Time (seconds)
Threshold (Mbps)
Action
Last Modified By
Last Modified Time
Options
* NTP_Reflection 30 4000 NONE Administrator Wednesday, April 8, 2015 Disable | Edit | Move Down
Name * NTP_Reflection
Description
This profile is used to monitor and detect unsolicited responses from NTP servers. The NTP servers responds to get monlist requests from a source that typically cannot be traced. The traffic is amplified and results in a huge amount of monlist query responses that consume the target's network resources and disrupt the network.
Large flow detection settings
L3 L3_PROTOCOL UDP
L4 UDP_SRC_PORT 123
Mitigation Settings
Observation Time (seconds) 30
Threshold (Mbps) 4000
Action NONE
* DNS_Reflection 15 5000 NONE Administrator Wednesday, April 8, 2015 Disable | Edit | Move Up | Move Down
* UDP_Attack 30 5000 NONE Administrator Wednesday, April 8, 2015 Disable | Edit | Move Up | Move Down
* ICMP_Flood 15 5000 NONE Administrator Wednesday, April 8, 2015 Disable | Edit | Move Up |

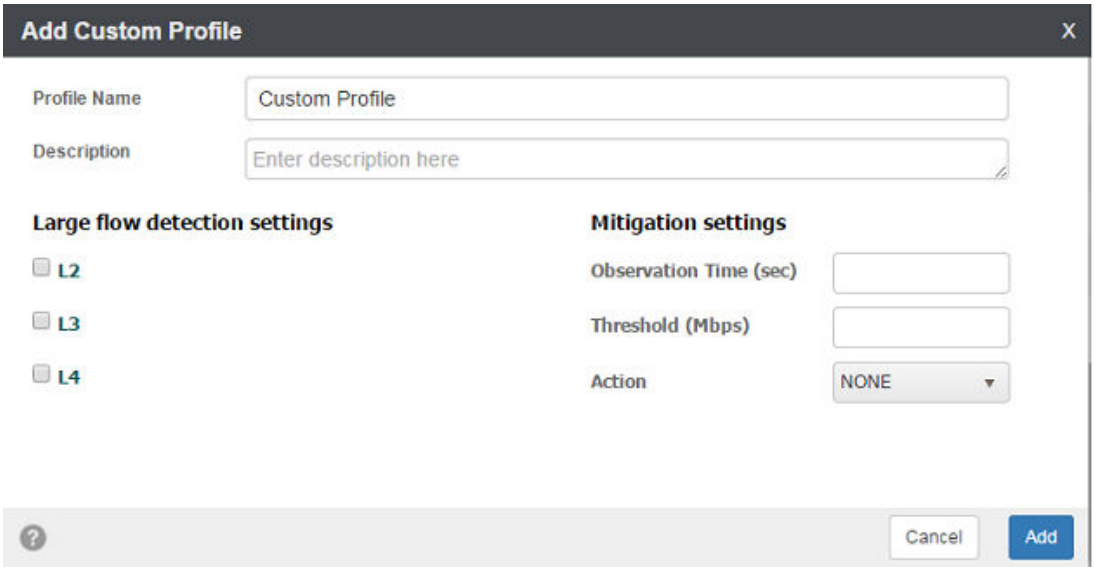
For information on how to enable or disable profiles and how to edit profiles, see:

- Enabling and Disabling Profiles on page 34
- Changing Large Flow Detection Parameter Settings on page 31
- Changing Mitigation Parameter Settings on page 32
- Changing the Priority of a Profile on page 33

## Add Custom Profile Dialog

You use the Add Custom Profile dialog to create new custom profiles. The dialog contains all of the options you need to configure the custom profile for use.

The following figure shows a blank Add Custom Profile dialog.

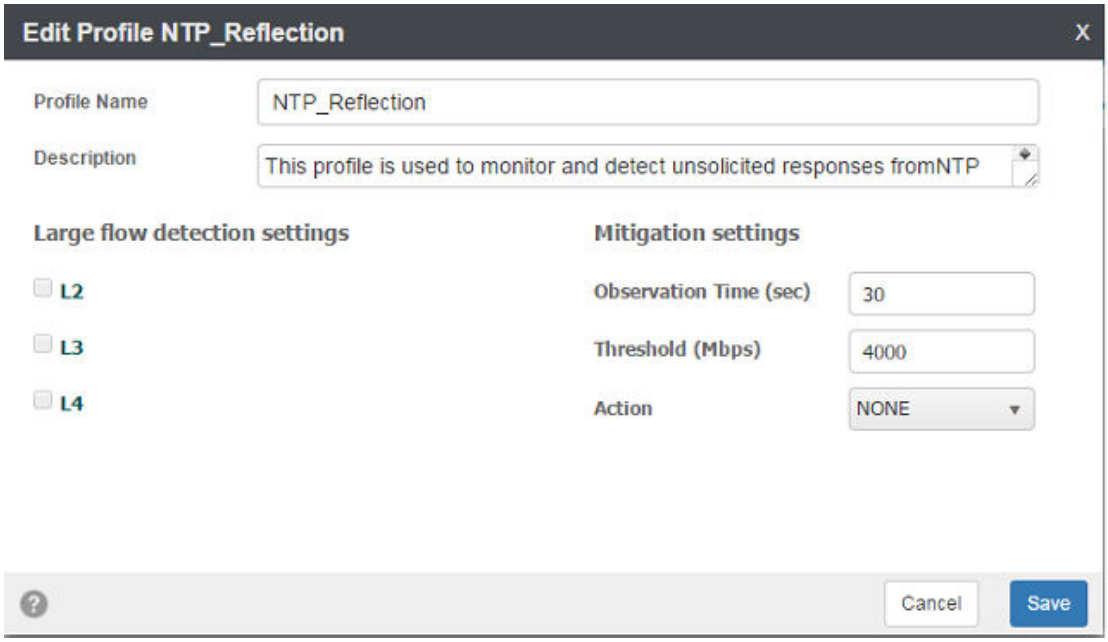



## Edit Profile Dialog

You use the Edit Profile dialog to edit existing profiles. The dialog contains all of the options you need to edit the profile as needed.

**NOTE**
You use this dialog to edit default profiles and custom profiles.

The following figure shows the Edit Profile dialog. In this example, the profile that has been selected for editing is the default profile named NTP_Reflection.



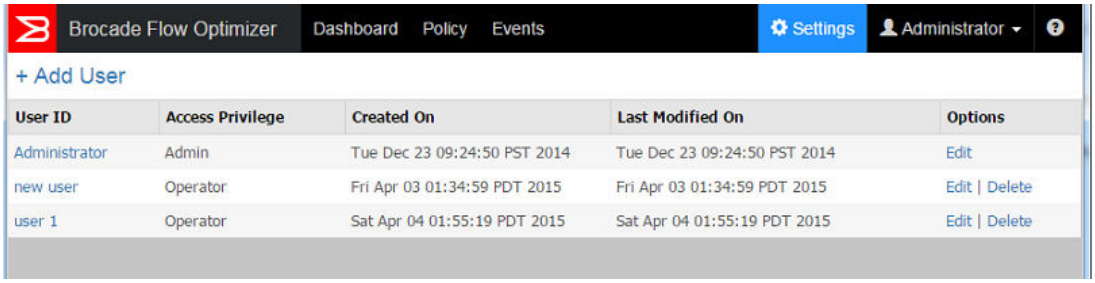

# Settings Page

The Settings page lists all system users. You use it to view current system users and to open the dialogs you use to manage system users. The types of user management actions you can perform varies depending on whether you have Administrator privileges or Operator privileges.

This table lists the user management actions that can be performed based on system privileges:

| Privileges | User Management Actions |
|---|---|
| Administrator | Add new users<br>Edit users<br>Delete users<br>Change their password or the passwords of users with Operator privileges |
| Operator | Change their own password (cannot change passwords of other users) |

The following figure shows the Setting page. In this example, 3 system users accounts have been defined (one Administrator and two Operator users).




## Add User Dialog

The Add User dialog is used to add new users to the system. You must have Administrator privileges to add new users.

**NOTE**
By default, all new users added by the Administrator have Operator privileges.

The following figure shows the Add User dialog.

## Edit User Dialog

The Edit User dialog is used to change passwords.

**NOTE**
If you are a user with Operator privileges, you can only change your password. If you are a user with Administrator privileges, you can change your password or the password of other users.

The following figure shows the Edit User dialog.

The application also enables Administrators to delete users and add new users.

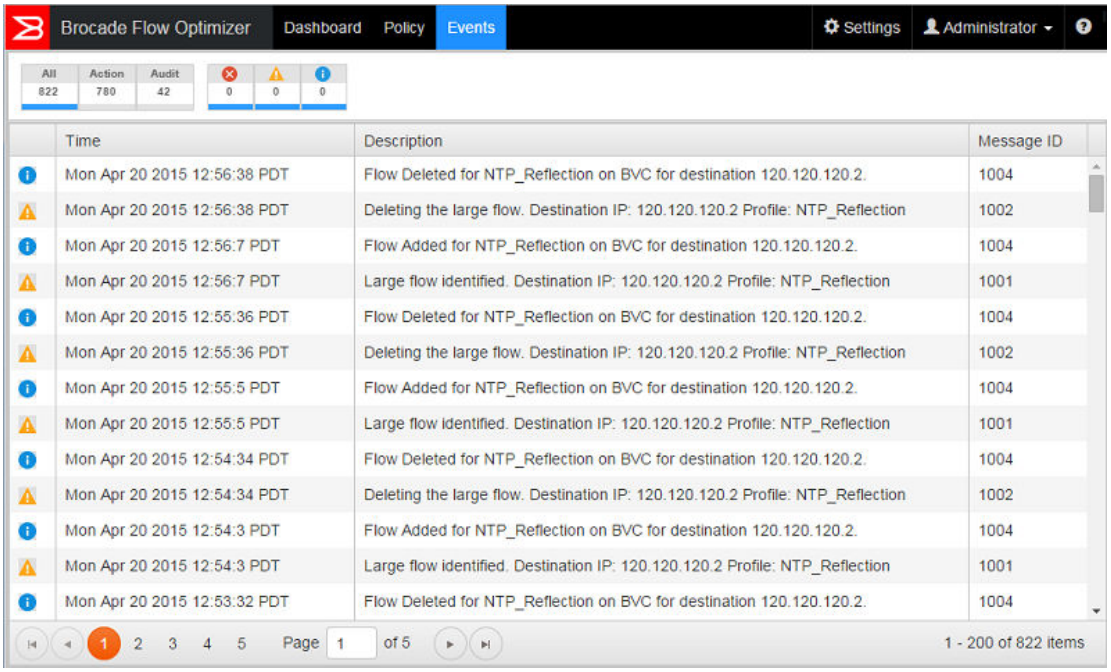
# Events Page

The Brocade Flow Optimizer provides real-time information for traffic monitoring events and audit events, which can be viewed in the Events page. The real-time events shown on the page have occurred over the last few days or more.

**NOTE**
The Events pane of the Dashboard provides the same real-time events information, but only for the last 30 minutes.

Events are listed in the table on the Events page, which is refreshed every 15 seconds. You can scroll through the list to view more events. If you scroll to the bottom of the table and want to view more events, click the pagination button to go to the next page.

The following figure shows the Events page.


Brocade Flow Optimizer
Dashboard
Policy
Events
Settings
Administrator
All 822
Action 780
Audit 42
0
0
0
Time
Description
Message ID
Mon Apr 20 2015 12:56:38 PDT
Flow Deleted for NTP_Reflection on BVC for destination 120.120.120.2.
1004
Mon Apr 20 2015 12:56:38 PDT
Deleting the large flow. Destination IP: 120.120.120.2 Profile: NTP_Reflection
1002
Mon Apr 20 2015 12:56:7 PDT
Flow Added for NTP_Reflection on BVC for destination 120.120.120.2.
1004
Mon Apr 20 2015 12:56:7 PDT
Large flow identified. Destination IP: 120.120.120.2 Profile: NTP_Reflection
1001
Mon Apr 20 2015 12:55:36 PDT
Flow Deleted for NTP_Reflection on BVC for destination 120.120.120.2.
1004
Mon Apr 20 2015 12:55:36 PDT
Deleting the large flow. Destination IP: 120.120.120.2 Profile: NTP_Reflection
1002
Mon Apr 20 2015 12:55:5 PDT
Flow Added for NTP_Reflection on BVC for destination 120.120.120.2.
1004
Mon Apr 20 2015 12:55:5 PDT
Large flow identified. Destination IP: 120.120.120.2 Profile: NTP_Reflection
1001
Mon Apr 20 2015 12:54:34 PDT
Flow Deleted for NTP_Reflection on BVC for destination 120.120.120.2.
1004
Mon Apr 20 2015 12:54:34 PDT
Deleting the large flow. Destination IP: 120.120.120.2 Profile: NTP_Reflection
1002
Mon Apr 20 2015 12:54:3 PDT
Flow Added for NTP_Reflection on BVC for destination 120.120.120.2.
1004
Mon Apr 20 2015 12:54:3 PDT
Large flow identified. Destination IP: 120.120.120.2 Profile: NTP_Reflection
1001
Mon Apr 20 2015 12:53:32 PDT
Flow Deleted for NTP_Reflection on BVC for destination 120.120.120.2.
1004
1 2 3 4 5
Page 1 of 5
1 - 200 of 822 items

For each event, the following information is provided in the columns of the Events page table:

- **Severity** The icon at the left of the table indicates the severity of the event.

| | |
|---|---|
| | Critical event |
| | Warning event |
| | Information event (system-wide events that occur during the processing of flows and application of mitigation actions) |

- **Time** The time the event occurred (the client time stamp).

- **Description** A brief description of the event.
- **Message ID** The unique identifier for the message.

The Events page also provides counters for real-time events.

| | |
|---|---|
| All | The total number of events that have been logged during the last 30 of the current session. |
| Action | The total number of events related to monitoring traffic for large flows. These events include the setup of profiles, flows, the detection of large flows, the execution of mitigation actions and more. |
| Audit | The total number of events performed by users (Administrator or Operator) that have been logged during the last 30 minutes of the current session. This includes the changing of controller settings, adding, editing, or deleting profiles, and user management events. |

# Troubleshooting

There are some basic procedures you can use to resolve issues you may encounter with the Brocade Flow Optimizer application database.

The troubleshooting steps cover these scenarios:

- If PostgreSQL Installed on Ubuntu on page 47
- If dbinitialization is triggered with permission denied error on page 47

**NOTE**
If you need to contact Support, make sure you have all the information you need to provide to Support (see The Process for Contacting Support on page 48).

# If PostgreSQL Installed on Ubuntu

Use this procedure to troubleshoot issues you may encounter with the Brocade Flow Optimizer application database. This procedure applies to systems in which PostgreSQL is running on Ubuntu.

Complete these troubleshooting steps:

1. Kill the PostgreSQL database service using port 5432 using these commands:

```
lsof -t -i :5432
kill -9 <pid>
```

2. Uninstall the existing Ubuntu PostgreSQL database using this command:

```
>> sudo apt-get remove --purge postgresql-9.x (where x can be either 1 or 3)
```

3. Restart the machine (mandatory).
4. Run this command in terminal for giving soft link:

```
ln -s /tmp/.s.PGSQL.5432 /var/run/postgresql/.s.PGSQL.5432
```

**NOTE**
If you receive the following error message, retry the command.

```
ln: failed to create symbolic link '/var/run/postgresql/.s.PGSQL.5432': File
exists
remove the PostgreSQL folder under /var/run and recreate the folder.
>> rm -rf /var/run/postgresql
>> mkdir /var/run/postgresql
```

# If dbinitialization is triggered with permission denied error

Use this procedure to troubleshoot issues you may encounter with the Brocade Flow Optimizer application database. This procedure applies to all system configurations.

Complete these troubleshooting steps:

1. Make sure the permissions assigned to the folder where the Brocade Flow Optimizer software is installed is set to **executable**.
2. If you need to change the permissions, use this command:

   **>> chmod 777 /<flowoptimizer_installation folder>/**.

# The Process for Contacting Support

When you need to contact Support to report an issue to Support, you need to complete a few tasks to ensure that you have all of the information needed to report the issue.

The tasks are:

- Generating Support Save Data on page 48
- (Optional)Changing the Logging Level on page 48
- Collecting Information to Report an Issue to Support on page 49

## Generating Support Save Data

When you report an issue to Support, you should provide support save data. This data includes details about the issue. You can easily generate the data using a script.

1. Go to the home directory for the application (where the application files were installed).
2. Open the bin folder.
3. Use one of the following commands to run the **supportsave** script.

   - **sh supportsave**
   - **./supportsave**

   The support save data is automatically saved to the home directory as a .tar file using this file (for example, *<flowoptimizer_home_directory>\data\supportsave\logs_<timestamp>.tar*).

**Next:**

- (Optional) You can change the logging level to enable debugging.
- Collecting Information to Report an Issue to Support

## Changing the Logging Level

When you report an issue to Support, you can enable the logging of debug messages by changing the logging level from INFO (logging of information) to DEBUG (debugging).

---

**NOTE**
This task is **optional**. You do not have to change the logging level to report an issue to Support.

---

**Pre-requisites:** Make sure you have generated support save data.

1. Go to the home directory for the application (where the application files were installed).
2. Open the configuration folder.
3. Open the *logback.xml* file in any text editor.
4. Enable debugging by changing the highlighted text in this example from INFO to DEBUG.

```
<logger name="com.brocade.dcm.apps.sdn.tsapp" level="INFO"
        additivity="false">
        <appender-ref ref="TSAPPFILE" />
        <appender-ref ref="STDOUT" />
</logger>

<logger name="com.brocade.dcm.apps.sdn.sflow.collector" level="INFO"
        additivity="false">
        <appender-ref ref="SFLOWCOLLECTORFILE" />
        <appender-ref ref="STDOUT" />
</logger>
```

5. Save the changes.
6. Restart the server.

**Next:** Collecting information to report an issue.

## Collecting Information to Report an Issue to Support

When you report an issue to Support, you need to collect certain information before you submit the report. Use this procedure to collect the information.

**Pre-requisites:** Make sure you have completed these tasks:

- Generating Support Save Data on page 48
- (Optional) Changing the Logging Level on page 48

1. Reproduce the issue.
2. Go to the directory where the support save data is stored (*<flowoptimizer_home_directory>\data \supportsave*/ ).
3. Make a copy the support save file (.tar) you generated in the previous task, and email it to Support.

**NOTE**
If you changed the logging level from INFO to DEBUG in a previous task, you must complete the remaining steps of this procedure. If you did not change the logging level from INFO to DEBUG, you have completed the tasks required to collect the information needed to report an issue to support.

4. Open the configuration folder (it is in the home directory).
5. Open the *logback.xml* file in any text editor.
6. Change the highlighted text (as shown in this example) from DEBUG to INFO.

```
<logger name="com.brocade.dcm.apps.sdn.tsapp" level="DEBUG"
        additivity="false">
        <appender-ref ref="TSAPPFILE" />
        <appender-ref ref="STDOUT" />
</logger>

<logger name="com.brocade.dcm.apps.sdn.sflow.collector" level="DEBUG"
        additivity="false">
        <appender-ref ref="SFLOWCOLLECTORFILE" />
        <appender-ref ref="STDOUT" />
</logger>
```

7. Save the changes.
8. Restart the application.

# Debugging Support

The Brocade Flow Optimizer provides a set of log files you can use for debugging purposes. The log files are installed automatically when you install the application software.

All of the log files are stored in the Logs folder in the home directory (the directory where the application files were installed). The following log files are provided:

| Log File | Use |
|---|---|
| *sflowcollector.log* | Used to record (log) sFlow data collection data. |
| *tsapp.log* | Used to record (log) mitigation action data (on the Controller). |
| *console.log* | Used to record (log) OSGi (Open Services Gateway initiative) container data. |
| *dbinit.log* | Used to record (log) database initialization data. |
| *sflowcollector.log* | Used to record (log) database service data. |

# Error Codes

The Brocade Flow Optimizer provides you with error messages for many of the issues you may encounter. You can use the information in the messages for troubleshooting purposes.

The types of error codes are:

- Common
- sFlow Collector
- sFlow persistence failure

- Application (Flow Optimizer)
- BVC Collector
- Profile validation
- Encryption

**NOTE**
Adjacent error codes may have numbers that are two or more whole numbers apart. This does not mean that an error code is missing. All of the current error codes are included.

## Common

The following table lists the common error codes and messages.

| Code | Message |
|---|---|
| 1000 | "Internal server error" |
| 1001 | "Database exception" |
| 1002 | "Exception while getting EventProfileInfos from database" |
| 1003 | "Exception while creating Event in database" |
| 1004 | "Name of profile is null or empty" |
| 1005 | "Exception while getting Profiles from database" |
| 1006 | "Failed to convert string to Errors object" |

## sFlow Collector

The following table lists the sFlow Collector error codes and messages.

| Code | Message |
|---|---|
| 2001 | "Invalid input parameters-granularity cannot be greater than duration" |
| 2002 | "Size of utilizations in database are not equal for populating or aggregating data" |
| 2003 | "Invalid username, username is null or empty" |
| 2004 | "Invalid password, password is null or empty" |
| 2005 | "Invalid username or password" |
| 2006 | "User does not exist" |
| 2007 | "Password encryption error" |
| 2008 | "User sessions have reached maximum limit" |
| 2009 | "Invalid token" |
| 2010 | "User does not have sufficient privileges" |
| 2011 | "Root user account cannot be deleted" |
| 2012 | "Duplicate user, the specified user already exists" |

| Code | Message |
|---|---|
| 2013 | "Root user account cannot be updated" |
| 2014 | "Invalid input parameters-start time is greater than end time" |
| 2015 | "Invalid Request, Attack Id is null or empty" |
| 2016 | "Invalid Request, Profile Id is null or empty" |
| 2017 | "Traffic flow detail is null" |
| 2018 | "Profile details is null" |

## sFlow persistence failure

The following table lists the sFlow persistence failure error codes and messages.

| Code | Message |
|---|---|
| 2500 | "DB: Attack Insertion failure for attack key {0} checksum {1}" |
| 2501 | "DB: Attack update failure for attack key {0} checksum {1}" |
| 2502 | "DB: Failed to move attack {0} to completion" |
| 2503 | "DB: Traffic Flow Insertion failure for checksum {0}" |
| 2504 | "DB: Timer series data 1sec update failure for checksum {0}" |
| 2505 | "DB: Failed to fetch Active Attacks from Database" |
| 2506 | "DB: Failed to purge entries for table {0}" |

## Application (Flow Optimizer)

The following table lists the application (Brocade Flow Optimizer) error codes and messages.

| Code | Message |
|---|---|
| 3001 | "The action {0} for flow {1} configuration is not supported" |

## BVC Collector

The following table lists the BVC Collector error codes and messages.

| Code | Message |
|---|---|
| 4001 | "Could not retrieve nodes from BVC" |
| 4002 | "Nodes from BVC are null or empty" |

## Profile validation

The following table lists the profile validation error codes and messages.

| Code | Message |
|---|---|
| 5001 | "Profile Name cannot exceed more than 128 characters" |
| 5002 | "Invalid Observation Interval value" |
| 5003 | "Invalid Threshold Value" |
| 5004 | "Invalid profile Type" |
| 5005 | "Invalid profile status" |
| 5006 | "Invalid user name" |
| 5007 | "Invalid mitigation action" |
| 5008 | "Priority already set. Please use different priority." |
| 5009 | "Network Attributes cannot be Empty" |
| 5010 | "Profile cannot have same network attribute twice" |
| 5011 | "Destination MAC cannot be empty." |
| 5012 | "Source MAC cannot be empty." |
| 5013 | "Source VLAN cannot be empty." |
| 5014 | "VLAN Priority cannot be empty" |
| 5015 | "IPv4 source address cannot be empty" |
| 5016 | "IPv4 destination address cannot be empty" |
| 5017 | "IPv6 source address cannot be empty" |
| 5018 | "IPv6 destination address cannot be empty" |
| 5019 | "IP Protocol cannot be empty" |
| 5020 | "DSCP cannot be empty" |
| 5021 | "TCP Source Port cannot be empty" |
| 5022 | "TCP Destination port cannot be empty" |
| 5023 | "UDP Source port cannot be empty" |
| 5024 | "UDP Destination port cannot be empty" |
| 5025 | "TCP Flags cannot be empty" |
| 5026 | "IP Fragment cannot be empty" |
| 5027 | "Invalid MAC Format. Please provide the MAC address in format 11:22:33:44:55:66" |
| 5028 | "Invalid IN VLAN String" |
| 5029 | "Invalid Vlan id. Valid Range: 0 to 4095" |
| 5030 | "Invalid VLAN Priority" |
| 5031 | "Invalid VLAN Priority. Valid Range: 0 - 7" |
| 5032 | "VLAN Id has to be selected for setting VLAN Priority" |
| 5033 | "Invalid IPv4 source address. Please enter valid IP address in CIDR format (eg: 10.5.6.7/32)" |
| 5034 | "Invalid IPv4 destination address. Please enter valid IP address in CIDR format (eg: 10.5.6.7/32)" |

| Code | Message |
|---|---|
| 5035 | "Invalid IPv6 source address. Please enter valid IP address in CIDR format (eg: 2001:cdba:9abc:5678::/64)" |
| 5036 | "Invalid IPv6 destination address. Please enter valid IP address in CIDR format (eg: 2001:cdba:9abc:5678::/64)" |
| 5037 | "Invalid IP Protocol. Valid values: TCP / UDP / ICMP" |
| 5038 | "Invalid DSCP. DSCP should be an integer value. Valid Range: 0 - 63" |
| 5039 | "IPv6 address cannot be selected when you want to set IPv4 source or destination" |
| 5040 | "IPv4 address cannot be selected when you want to set IPv6 source or destination" |
| 5041 | "The IP Protocol must be set to TCP when TCP Port is selected" |
| 5042 | "UDP Port cannot be selected when TCP port is selected" |
| 5043 | "The IP Protocol must be set to UDP when UDP Port is selected" |
| 5044 | "TCP Port cannot be selected when UCP port is selected" |
| 5045 | "The IP Protocol must be set to TCP when TCP Flag is selected" |
| 5046 | "Invalid TCP flag. Valid values: URG / ACK / PSH / RST / SYN / FIN" |
| 5047 | "Only yes / No is allowed for IP fragment option" |
| 5050 | "When redirect action selected, please provide the redirect node and port" |
| 5051 | "Invalid Redirect node or port. Valid Format MAC: aa:bb:cc:dd:ee:ff Port: 1,2" |
| 5052 | "The profile name\" {0} \"from query parameter and profile name \" {1} \" from profile object does not match" |
| 5053 | "Failed to search user name for given user ID" |
| 5054 | "Failed to insert profile {0}" |
| 5055 | "Failed to insert mitigation association {0} {1}" |
| 5056 | "Failed to insert profile attribute association {0} {1} {2}" |
| 5057 | "Failed to delete the profile {0}" |
| 5058 | "Failed to update profile {0}" |
| 5059 | "Failed to delete Profile Mitigation Association for profile {0}" |
| 5060 | "Failed to delete profile attribute association for profile {0}" |
| 5061 | "Unable to retrieve nodeId for node: {0} from BVC" |
| 5062 | "Failed to create flow request. Profile Name: {0} Action: {1} Flow Key {2}" |
| 5063 | "Failed to Program Flow for {0} on BVC for node: {1} for destination {2}" |
| 5064 | "Failed to Create meter for {0} on BVC for node: {1} for VLAN {2}" |
| 5065 | "Failed to Program Flow for {0} on BVC for node: {1} for VLAN {2}" |
| 5066 | "Failed to Delete meter for {0} on BVC for node: {1} for VLAN {2}" |
| 5067 | "Failed to get configured nodes for programming flow: {0}" |
| 5068 | "Failed to Create meter for {0} on BVC for node: {1}" |

| Code | Message |
|---|---|
| 5069 | "Failed to validate IP address {0} during the attack detection" |
| 5070 | "Please select NONE as an action when detection only parameters are selected" |
| 5078 | "Invalid Profile Name. Only Alphanumeric, spaces and following special characters (- / . / _ / ~) are allowed" |

## Encryption

The following table lists the encryption error codes and messages.

| Code | Message |
|---|---|
| 6001 | "Error while initializing the PBE security key" |
| 6002 | "Error while encrypting the text" |
| 6003 | "Error while decrypting the text" |